WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Enhancing Cybersecurity Using Artificial Intelligence: An Analysis of Neural Network and Machine Learning Algorithms"

*Mohammadreza Chizari*

**Bachelor's Degree Computer Engineering, Islamic Azad University, mhmdrezachizari@gmail.com**

Doi : https://doi.org/10.55248/gengpi.5.0924.2625

**ABSTRACT**

In today's era, where technology is developing rapidly, cyber security has become one of the most critical issues for organizations, governments and even individuals. Cyber security is not only about protecting our data and systems from cyber attacks, but also about protecting our privacy, financial information and identity. Meanwhile, artificial intelligence (AI) as a powerful and transformative tool plays an essential role in strengthening cyber security. Cyberattacks can easily attack computer systems and information networks and cause problems such as information theft, data destruction, damaging systems and many more. In this context, applying artificial intelligence to improve cyber security can be useful. Artificial intelligence in cyber security serves various purposes including threat detection, threat hunting, threat intelligence and incident response Among the widely used AI techniques in threat detection are anomaly detection, natural language processing (NLP), random forests, and graph analysis. In this research, the applications of artificial intelligence in cyber security and how to use it to improve the security of systems and networks have been investigated.

**Keywords**: cyber security, artificial intelligence, neural networks, machine learning.

## Introduction

Artificial intelligence, as one of the advanced technologies, is capable of automatically and intelligently identifying, predicting and preventing cyber attacks. By analyzing big data and using complex algorithms, this technology can help identify suspicious patterns in user behavior, identify system weaknesses, and predict cyber attacks. Artificial intelligence, with its unique capabilities, including machine learning and natural language processing, has created a revolution in the field of cyber security. The use of artificial intelligence in this field allows organizations to use big data to detect, analyze and respond to cyber threats in a faster and more accurate way. This technology is able to identify complex patterns in data, even if these threats have not been seen beforeIn other words, artificial intelligence can help discover new attacks or Zero-Day Attacks. This is very important; Because hackers are constantly developing new ways to break into systems. Cyber security is a constantly evolving field, and the use of artificial intelligence (AI) in cyber security is a relatively new but rapidly growing field of research and application. In today's digital world, cyber security has become one of the most important challenges and basic needs of organizations and individuals. With the increase in the number and complexity of cyber attacks, the need for more advanced and smarter solutions to deal with these threats is felt more and more. Artificial intelligence, as one of the advanced technologies, plays a very important role in improving cyber security In this article, we will examine the applications of artificial intelligence in cyber security and how to use it to improve the security of systems and networks.

## Theoretical Foundations

### Artificial Intelligence

Artificial intelligence (AI) is the ability of computer systems to perform tasks that normally require human intelligence, such as learning, reasoning, and problem solving. This is achieved by using sophisticated AI algorithm models to process and analyze large amounts of data. A trained AI model uses patterns and insights discovered from data to perform tasks such as predicting and generating output.

Artificial Intelligence Algorithm: An artificial intelligence algorithm is a set of instructions that defines how an artificial intelligence system processes data. For example, the CNN (Convolutional Neural Network) algorithm defines how visual images are analyzed by an artificial intelligence system.

Artificial Intelligence Model: An artificial intelligence model is a trained instance of an algorithm that collects the learned knowledge and uses it to perform tasks. For example, a trained CNN model is used to recognize and classify new and unseen images. (Ahmadi, Sunti,2023).

### Machine Learning

Machine learning is a branch of artificial intelligence that allows computers to learn patterns from data without direct programming and to make decisions based on them. In machine learning, algorithms automatically learn from input data and with their help they find the ability to predict and analyze new data. Machine learning is generally a combination of mathematical optimization and statistics. This function is at the peak of its popularity today. This is because of its many attractive applications, such as speech recognition, search, recognition of behavioral patterns and relationships in social networks, recommendation algorithms (like what is in Instagram or Netflix), computer vision, etc. Machine learning (ML) and artificial intelligence are often discussed as if they are separate technologies, but they are not. In fact, ML is a specific approach in artificial intelligence that focuses on enabling machines to learn and improve from experience without explicit programming. Instead of providing precise instructions, ML algorithms learn patterns in large volumes of data to make predictions or decisions. Artificial intelligence is a broader concept that encompasses the entire field of developing intelligent machines. while ML acts as an important component in artificial intelligence and provides a tool for machines to achieve artificial intelligence. (Keshavarz, Hosseini,2023)

## Cyber security

History of artificial intelligence in cyber security

In the beginning, artificial intelligence was mostly used in the form of basic intrusion detection systems (IDS) and intrusion prevention systems (IPS). These systems were mainly based on rules defined by security experts and were able to identify known threats based on specific signatures. However, with the development of threats and the evolution of attack methods, the need for more advanced and flexible methods was felt. In the 1990s, with significant developments in the field of machine learning and artificial intelligence algorithms, we saw the use of newer techniques in cyber security. These techniques allowed the detection of complex and unknown patterns that were previously hidden from older systems. In the early 20th century, with the increasing growth of big data and increasing computing power, artificial intelligence entered a new stage. The use of deep learning (Deep Learning), which is a subset of machine learning, made it possible to process and analyze a huge amount of cyber data. These advances enabled security systems to automatically detect complex and emerging threats with high accuracy (Ahmadi, Santi,2023).

Today, artificial intelligence is not only used in detecting and predicting cyber threats, it is also used in developing preventive security solutions and building systems that are able to learn and adapt to new threats. From intelligent intrusion detection systems to security tools designed using machine learning to identify suspicious behavior in networks, all of them show how artificial intelligence has been able to add new dimensions to the field of cyber security. (Malik,2023)

## Discussion

Cyber security with artificial intelligence

Using advanced algorithms, artificial intelligence can help detect cyber attacks automatically and in the shortest possible time. By analyzing huge amounts of data, AI can examine network traffic patterns and detect any attacks. Also, by using neural networks, artificial intelligence can automatically predict the suspicious behavior of users and notify him if necessary. Also, AI can improve cyber security by using big data analysis. By analyzing big data, it is possible to identify suspicious patterns in the behavior of users and systems and, if necessary, to close access to suspicious data.

**How artificial intelligence works in cyber security**

Artificial intelligence combines large data sets and uses them with visual processing algorithms. As the scope of networks and systems expands, artificial intelligence in cybersecurity helps automate operations by processing large amounts of data much faster than a human. For this reason, most cybersecurity tools integrate deep learning and other capabilities designed to work with big data.

Artificial intelligence can help improve cybersecurity in several different areas:

Threat detection: AI algorithms can help identify unusual patterns in data and network traffic and automatically detect cyber threats.

Attack prediction: By analyzing past data and using machine learning techniques, artificial intelligence can predict future cyber attacks and suggest preventive measures.

Data analysis: AI can quickly analyze la Automating security processes: by using artificial intelligence, many security processes can be done automatically, which leads to increased efficiency and reduced human errors.

Volume of data and extract useful information that helps improve the security of systems.

**Detect and respond to cyber threats**

One of the most important applications of artificial intelligence in cyber security is to detect and respond to cyber threats. Machine learning algorithms can detect unusual patterns in network traffic and user behavior and automatically respond to threats. For example, AI-based intrusion detection systems (IDS) can detect DDoS attacks, unauthorized intrusions, and malicious activities and take necessary actions to counter them. (Malik,2023)

**Analysis and prediction of cyber attacks**

Artificial intelligence can predict future cyber attacks by analyzing past data and using predictive techniques. This allows organizations to take proactive measures to counter potential threats. For example, machine learning algorithms can identify phishing attack patterns and alert users.

**Security data analysis**

Artificial intelligence can quickly analyze large volumes of security data and extract useful information that helps improve the security of systems. For example, data analysis algorithms can analyze system logs and identify unusual patterns that may be indicative of a cyber attack.

**Automation of security processes**

With the use of artificial intelligence, many security processes can be automated, which leads to increased efficiency and reduced human errors. For example, AI-based security information management (SIEM) systems can automatically detect threats and take necessary actions to counter them.

**Authentication and access management**

Artificial intelligence can help improve authentication and access management processes. For example, AI-based multi-factor authentication systems can use biometric techniques such as facial recognition and fingerprints to authenticate users Also, artificial intelligence algorithms can analyze user behavior and identify unauthorized access.

**Countering phishing attacks**

Phishing attacks are one of the most common and dangerous cyber threats. Artificial intelligence can help identify and counter these types of attacks. For example, machine learning algorithms can detect phishing emails and alert users. Also, AI-based systems can identify phishing websites and block access to them.

**Analysis of user behavior**

Artificial intelligence can analyze user behavior and identify unusual patterns that may be a sign of a cyber threat. For example, machine learning algorithms can analyze user behavior in real time and automatically respond to threats. This allows organizations to quickly respond to threats and prevent attacks from occurring.

**Vulnerability management**

Artificial intelligence can help identify and manage system vulnerabilities. For example, data analysis algorithms can identify vulnerabilities in software and systems and notify security managers. Also, artificial intelligence-based systems can automatically apply security updates and prevent the exploitation of vulnerabilities. (Deibert Rohozinski, 2010)

**Network traffic analysis**

Artificial intelligence can analyze network traffic and identify unusual patterns that may be a sign of a cyber attack. For example, machine learning algorithms can analyze network traffic in real time and automatically respond to threats. This allows organizations to quickly respond to threats and prevent attacks from occurring.

**Analysis of system logs**

AI can analyze system logs and identify unusual patterns that may be a sign of a cyber attack. For example, data analysis algorithms can automatically analyze system logs and notify security administrators. This allows organizations to quickly respond to threats and prevent attacks from occurring.

## Limitations of using artificial intelligence in cyber security

Complexity of algorithms: AI algorithms are usually complex and require a lot of computing resources. This can increase the costs of implementing and maintaining AI-based systems.

Need for big data: AI algorithms need big data to train and improve their accuracy. Collecting and managing this data can be challenging and require a lot of resources and time.

Security risks: The use of artificial intelligence in cyber security can automatically create new security risks. For example, attackers can target AI algorithms and manipulate them to achieve their goals.

Need for expertise: Implementing and managing artificial intelligence-based systems requires expertise and technical knowledge. This can be challenging and requires the training and hiring of specialized personnel. (Malik,2023)

Algorithmic Errors: AI algorithms may make errors and provide incorrect results. This can lead to misidentification of threats and wrong actions to counter them. . (Deibert Rohozinski, 2010)

## Machine learning in cyber security

Artificial intelligence and cyber security are connected today more than ever. The demand and demand for people who have skills and abilities in both fields is very high today. Companies and technology organizations are looking for people who understand both cybersecurity and artificial intelligence well enough to know when and how to use artificial intelligence techniques in their cybersecurity processes. Data scientists, analysts and engineers who have experience and expertise in the field of cyber security are very much needed. To fulfill these responsibilities, it is necessary to have knowledge and experience in fields such as data modeling in machine learning, advanced neural networks, linguistic modeling, and behavior analysis; In addition, they must have a good understanding of the principles of cyber security

An AI cybersecurity specialist should have strong knowledge in the areas of network security, computer forensics and cryptography, malware detection and defense, as well as data protection. Developing AI in cyber security requires in-depth knowledge of machine learning, deep learning, natural language processing (NLP), data analysis, as well as security skills such as intrusion detection, cryptography, and threat analysis.

The importance of machine learning in cyber security is undeniable. Fortunately, machine learning can help solve the most common tasks, including pattern recognition, prediction, regression, and classification. It seems that in an era with a large amount of data and a shortage of network security professionals, machine learning is an alternative solution to many problems. In fact, through machine learning, millions of files can be sorted to detect threats

For example, Microsoft Windows Defender uses multiple layers of machine learning to prevent potential threats (Dunn Cavelty, 2008).

The main methods of machine learning

Supervised learning

In supervised learning, algorithms are trained on a set of training data that includes inputs and outputs associated with them. The goal of this method is to find a function that can produce appropriate outputs based on new inputs. Examples of supervised learning algorithms include:

• Linear regression

• Decision tree

• Artificial neural networks

Unsupervised learning

In unsupervised learning, algorithms work with data that does not have a specific label or output. The purpose of this method is to discover hidden patterns and relationships in the data. Examples of unsupervised learning algorithms include:

• Clustering

• Dimension reduction

• Reinforcement learning

Signature-based threat detection

Older threat detection systems use heuristic and static signatures to detect threats and anomalies. For example, antiviruses create and maintain a database of virus signatures based on the characteristics of the virus program. Then they compare the virus program with the signatures in the database and identify and remove it. (Deibert Rohozinski, 2010)

Although signature-based threat detection technology is easy to understand, it is not a powerful method. One of its biggest problems is that because in this method each packet must be compared with all the signatures in the database, when the size and speed of the data stream increases significantly, it cannot be ensured that the signature comparison process matches the data input speed. If synchronization is not maintained, it is possible Part of the database is left out. Today, signature-based systems are gradually being replaced by intelligent cyber security agents. Machine learning has made positive progress in this field by identifying new types of malware, zero-day attacks, and advanced persistent threats.

**Advanced Persistent Threats**

Attacks are generally difficult to prevent due to their complex nature. Machine learning can detect the attack in the early stages and prevent it from spreading to the entire system. Many network security companies use machine learning to detect APT attacks in the early stages of a threatThis method effectively prevents identity data leakage and internal threats. Prescriptive analytics perform better in this field. This type of analysis determines what measures should be taken to minimize losses after a cyber attack. (Malek,2023)

**Performance Adjustment and Error Detection**

Performance tuning and fault detection are the most important repetitive processes of a machine learning system that can help improve system performance. If the generalization function of the system can have a lower generalization error with a higher probability, it can be said that the system has a good performance. Every day, more and more companies are using machine learning to keep their modern IT environments secure.

**Vulnerability Scanning**

Machine learning is also used to scan networks for vulnerabilities and automate processes. Almost all cybersecurity companies use machine learning in their products to identify and protect against threats. The role of machine learning in network security is to identify behavior patterns of users, data, equipment, systems and networks and to distinguish abnormal from normal. Machine learning also helps managers to analyze a lot of data, investigate new types of threats and respond to threats faster. (Ahmadi, Santi, 1402)

**Company Security**

Humans are an important and diverse carrier of cyber risks (from insider threats and abuse of privileges and management to hackers). Therefore, machine learning helps to detect changes in the way users interact in the IT environment and describe their behavioral characteristics in the attack environment. Despite the high marketing requirements, the reality is that the enterprise security environment is a huge and dynamic network

And managers must constantly monitor this network and review and update data based on unpredictable and persistent internal and external threat vectors. Although machine learning offers various advances in the ability to detect, investigate and respond to threats, it is the combination of personnel and technology that can handle a wide range of threats in the evolving security environment. (Malik,2023)

## Conclusion

Artificial intelligence, as one of the advanced technologies, plays a very important role in improving cyber security. Using artificial intelligence algorithms, organizations can automatically detect and respond to cyber threats, predict future cyber attacks, analyze security data, and automate security processes. Now, the use of artificial intelligence in cyber security comes with challenges and limitations that need to be managed and resolved. Considering the importance of cyber security in today's digital world, the use of artificial intelligence can help organizations improve the security of their systems and networks and prevent cyber attacks. Artificial intelligence, using deep learning algorithms and big data analysis, is able to recognize emerging and complex patterns that traditional methods cannot detect. This technology adapts its defense strategies to counter new attacks by continuously analyzing data and learning from past experiences. Developing AI in cyber security requires in-depth knowledge of machine learning, deep learning, natural language processing (NLP), data analysis, as well as security skills such as intrusion detection, cryptography, and threat analysis. In order to prevent training data poisoning, it is necessary to carefully evaluate and refine the input data. It is essential to use data validation mechanisms and regularly review data to identify unusual patterns or manipulated data; Also, training AI models using diverse data from reliable sources helps to reduce the possibility of poisoning.

**Resources**

Ahmadi, Seyyed Ali Akbar and Saneti, Iman, 2023, cyber security and information preservation using artificial intelligence, the fourth national conference on new challenges and strategies in electrical and computer engineering in Iran, Bandargaz, https://civilica.com/doc/2021879

Keshavarz, Zahra and Hosseini, Hamidreza, 2023, Artificial intelligence in cyber security (applications, challenges and opportunities), 6th National Conference of New Technologies in Electrical, Computer and Mechanical Engineering of Iran, Tehran, https://civilica.com/ doc/1744302

Malek, Hadi, 2023, Providing Cyber Security in Iran: Challenges and Solutions, The Fourth National Cyber Defense Conference, Maragheh, https://civilica.com/doc/1917265

Jafari Zhandei, Nooruddin, 1403, JCDC Cyber Security and Defense Analysis, https://civilica.com/doc/1982543

Deibert, R. and Rohozinski, R. (2010) 'Risking Security: Policies and Paradoxes of Cyberspace Security', International Political Sociology 4 / 1: 15–32. An intelligent account of the threat discourse that differentiates between risks to cyberspace and risks through cyberspace.

The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World, Cabinet Office, London, UK, available at https://update.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategyfinal. pdf (accessed on May 5, 2012).

Dunn Cavelty, M. (2008), Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, London: Routledge. Examines how, under what conditions, by whom, for what reasons, and with what impact cyber-threats have been moved on to the political agenda in the USA.

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, The White House, Washington DC, USA, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed on May 5, 2012)